ABSTRACT

A method includes hooking a critical operating system function, stalling a call to the critical operating system function originating from a call module, determining a location of the call module in a kernel address space of a memory, and determining whether the location is in a driver area of the kernel address space. Upon a determination that the call module is not in the driver area, the method further includes taking protective action to protect a host computer system. In this event, it is highly likely that the call module is malicious code that has been injected into the kernel stack/heap through a malicious kernel mode buffer overflow attack. By taking protective action, exploitation, damage or destruction of the host computer system is prevented.